

CLAIMS

1. A system for addressing denial of service attacks directed at a web resource, comprising:
 - a system for detecting improper requests; and
 - a system for responding to improper requests that issues an HTTP “OK” response code when improper request is detected.
2. The system of claim 1, wherein the system for responding stops issuing HTTP “OK” response codes and issues no response after a predetermined number of improper requests are detected.
3. The system of claim 1, wherein a request is deemed improper if the request is received from an unexpected host.
4. The system of claim 1, wherein a request is deemed improper if the request has a zero length.
5. The system of claim 1, wherein a request is deemed improper if an HTTP “post” or an HTTP “get” command is expected and neither an HTTP “post” nor an HTTP “get” command is received.

6. The system of claim 1, wherein a request is deemed improper if the request includes a HTTP “post” or “get” command with unknown arguments.
7. The system of claim 1, wherein the HTTP “OK” response code comprises an HTTP 204 “OK” message code.
8. The system of claim 1, wherein the system for responding to improper requests includes a response protocol that utilizes a standard error handling procedure for a first improper request from a requesting resource, issues an HTTP OK response code for N subsequent improper requests from the requesting resource, and then stops responding to the requesting resource altogether.
9. The system of claim 1, wherein the web resource comprises a server.

10. A method for addressing denial of service attacks directed at a web resource, comprising:

- receiving messages at the web resource;
- analyzing each message and determining if the message is improper;
- storing the source address of a message if the message is improper;
- responding to a first improper message from an identified source address with an HTTP error response;
- responding to a set of subsequent improper messages from the identified source address with HTTP “OK” response codes; and
- stopping responses to the identified source address for all received improper messages after the set of subsequent improper messages have been responded to.

11. The method of claim 10, wherein a message is deemed improper if the message is received from an unexpected host.

12. The method of claim 10, wherein a message is deemed improper if the message has a zero length.

13. The method of claim 10, wherein a message is deemed improper if the message is neither an HTTP “post” nor an HTTP “get” command when one of these commands is expected.

14. The method of claim 10, wherein a message is deemed improper if the message includes a HTTP "post" or "get" command with unknown arguments.
15. The method of claim 10, wherein the HTTP "OK" response code comprises an HTTP 204 "OK" message code.
16. The method of claim 10, wherein the HTTP "OK" response comprises an HTTP 200 "OK" message code.

17. A program product stored on a recordable medium for addressing denial of service attacks directed at a web resource, comprising:

means for receiving messages at the web resource;

means for analyzing each message and determining if the message is improper;

means for storing the source address of a message if the message is improper;

means for responding to a first improper message from an identified source address with an HTTP error response; and

means for responding to subsequent improper messages from the identified source address with HTTP “OK” response codes.

18. The program product of claim 17, further comprising means for stopping responses to the identified source address after a predetermined number of subsequent improper messages have been received.

19. The program product of claim 17, wherein a message is deemed improper if the message is received from an unexpected host; if the message has a zero length; if the message is neither an expected HTTP “post” nor an expected HTTP “get” command; or if the message includes a HTTP “post” or “get” command with unknown arguments.

20. The program product of claim 17, wherein the HTTP “OK” response codes comprise HTTP 204 “OK” response codes.

21. The program product of claim 17, wherein messages that are deemed proper are passed to the web resource for further processing.
22. The program product of claim 17, wherein the web resource is a web server.